REMARKS

The Examiner has revised the current rejection in light of new prior art and a reformulated rejection. As set forth below, such new rejection is deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of multiple dependent claims into each of the independent claims. Since the subject matter of such dependent claims was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has rejected Claims 1-7, 9-10, 14-18, 24, 26-31, 33-34, 38-42, 44, 50, and 53-54 under 35 U.S.C. 103(a) as being unpatentable over Muttik (U.S. Patent No. 6,775,780) in view of Bowlin (U.S. Patent Application No. 2002/0099944). The Examiner has also rejected Claims 19, 21-23, 43, 45-47, 51 and 52 under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Bowlin in further view of Schnurer (U.S. Patent No. 5,842,002). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With regard to independent Claims 1, 24, and 50-52, the Examiner has relied on the following excerpts from Muttik and Bowlin in addition to Figure 6 in Bowlin to meet applicant's claimed "running a computer on a network in an opened share mode, wherein the opened share mode indicates a file structure parameter and a name parameter and applies only to a manually selected list of at least one of application programs and data" (see Claims 1, 24 and 50) and "running a computer on a network in a virtual opened share mode and an actual opened share mode" (see Claims 51 and 52).

> "**Computer system 106 receives code 108 (which can potentially be malicious) from a number of different sources.** Code 108 may be introduced into computer system 106 by a remote host 101 across a network 102. For example, code 108 may be included in an electronic mail (email) message from remote host 101 to computer system 106. Remote host 101 can be any entity that is capable of sending code 108 across network 102. Network 102 can include any

type of wire or wireless communication channel capable of coupling together computing nodes. This includes, but is not limited to, a local area network, a wide area network, or a combination of networks. In one embodiment of the present invention, network 102 includes the Internet." (Muttik Col. 3, lines 30-42-emphasis added)

"To make the selections for the safe zone, the user may be presented with a display screen 600 such as the one illustrated in FIG. 6. The display screen 600 may, for example, mimic an operating system's own method of displaying files and directories to a user (e.g., Microsoft.RTM.'s Windows Explorer). **The user may be able to select files and/or entire directories for the safe zone** by simply marking the check boxes (e.g., 610, 620 and 630) which are associated with files and directories presented on the computer display screen 104. The check boxes may be marked using an appropriate input device 310 associated with the computer system 100 (e.g., mouse 108, keyboard 106, pen tablet, touch screen, or trackball). For example, FIG. 6 shows that the user has selected for the safe zone two individual files (FILE1 and FILE2) and an entire directory (PROJECTS) by marking the check boxes 610, 620 and 630. Alternatively, other methods of selecting the files and/or directories to be included in the safe zone are possible. For example, the selections could be made by the user uttering voiced responses." (Bowlin [0038]-emphasis added)

Applicant respectfully asserts that the above excerpts fail to meet applicant's claimed, "wherein the opened share mode indicates a file structure parameter and a name parameter and applies only to a manually selected list of at least one of application programs and data" (see Claims 1, 24 and 50) and "running a computer on a network in a virtual opened share mode and an actual opened share mode" (see Claims 51 and 52). Specifically, Muttik simply discloses a "[c]omputer system 106 receives code 108 (which can potentially be malicious) from a number of different sources" (see emphasized excerpt above), which completely fails to even mention any opened shared mode, and especially not an actual opened share mode and a virtual opened share mode, in the context of applicant's claim language.

Further, Bowlin simply discloses that "[t]he user may be able to select files and/or entire directories for the safe zone" (see emphasized excerpt above). Applicant argues that "select[ing] files and/or entire directories for the safe zone" where a first database "identifies files stored on the computer to be included in a safe zone...[and]...a second database...defines authorized accesses to the files within the safe zone" (see Bowlin

Abstract) *teaches away* from applicant's claimed "opened share mode," both virtual and actual, since Bowlin's selected files are not part of an opened share but instead have restricted (not open) access.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 9 into each of the independent claims and the subject matter of Claim 54 into independent Claims 1, 24 and 50.

With respect to the subject matter of former Claim 9 et al., now incorporated into each of the independent claims, the Examiner relies on the above cited excerpt from Bowlin (paragraph [0038]) to meet applicant's claimed "wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection." The Examiner further states that "Bowlin describes a system where the user randomly selects the parameters which are incorporated as being in the open share mode."

Applicant respectfully asserts that Bowlin does not teach random selection as claimed by applicant. Specifically, Bowlin simply teaches that "[t]he user may be able to

select files and/or entire directories for the safe zone" (see emphasized excerpt above [0038]). There is simply no disclosure of such selection being "random." Furthermore, Bowlin also fails to teach random selection "to prevent detection," as claimed by applicant. Bowlin's selection of files is with regards to a "safe zone" that has certain access limitations (see Bowlin Abstract), and not to prevent detection.

With respect to the subject matter of former Claim 54, now incorporated into independent Claims 1, 24 and 50, the Examiner relies on the following excerpt from Bowlin to meet applicant's claimed "wherein the computer is run in an actual opened share mode and a virtual opened share mode such that the at least one of application programs and data is accessible in the actual opened share mode, and attempted access to the at least one of application programs and data associated with the virtual opened shared mode prompts a security process":

> "As shown in FIG. 2, the method 200 generally comprises the following steps. In the first step 202 of method 200, **the user selects what files (e.g., file 420) stored on the computer system 100 will be included in a safe zone and selects authorized accesses (e.g., application accesses, process accesses, service accesses, system agent and user accesses, etc.) to the files within the safe zone.** Assuming that a request to access a file is made (step 204), a filter 306 determines at step 206 whether the file to be accessed is within the safe zone. If the requested file is determined to be not within the safe zone, access to the file is granted in step 208. However, if the file is determined to be within the safe zone, a determination is made at step 210 as to whether the request is authorized. If the request is determined to be authorized, access to the file is granted at step 208. But if the request is determined to be unauthorized, access to the file is denied (step 212)." (Bowlin [0026]-emphasis added)

Applicant respectfully asserts that Bowlin does not teach "an actual opened share mode and a virtual opened share mode" (emphasis added). Specifically, Bowlin teaches "the user selects what files...will be included in a safe zone and selects authorized accesses...to the files within the safe zone" (see emphasized excerpt above), which clearly does not disclose "an actual opened share mode and a virtual opened share mode."

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

The Examiner's rejections are further deficient with respect to the dependent claims. For example, with respect to dependent Claim 5 et al., the Examiner relies on Bowlin's disclosure of an "application obtain[ing] access to a file" ([0035]) and "program code for allowing the user to designate which files or directories within the safe zone each authorized application, process, user, etc. is allowed to access" ([0044]). Applicant respectfully asserts that teaching a method of an application obtaining access to a file and of limiting access to a file, as in Bowlin, does not meet a "virtual opened share mode" nor "modifying an application program interface," as claimed by applicant.

In addition, the Examiner has rejected Claim 55 under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Bowlin in further view of Schnurer and in further view of Porras (U.S. Patent No. 6,704,874). Applicant respectfully disagrees with such rejection.

With respect to dependent Claim 55, the Examiner relies on Muttik's disclosure of a "system [that] records system calls (API calls) generated by code" to meet applicant's claimed "recording in a record information on any attempt to modify the computer including time and source information" (Col. 4, lines 32-44). Applicant respectfully asserts that simply recording system calls, as taught in Muttik, does not meet applicant's specific claim of "recording...any attempt to modify the computer including time and source information" (emphasis added).

In addition, the Examiner relies on Muttik's disclosure of "determining whether software is likely to exhibit malicious behavior by analyzing patterns of system calls" (see Abstract) and Muttik's Figure 1 to meet applicant's claimed "logging the computer back on the network in a mode other than the actual opened share mode." Applicant respectfully asserts that the excerpts and Figure relied on by the Examiner do not make any suggestion of logging a computer back on a network in a mode other than the actual

opened share mode. In fact, the above reference does not even teach logging back on the network in any mode, let alone in a mode other than the actual opened share mode.

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a specific prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims depending therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P019).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100